IN THE SUPREME COURT OF GEORGIA

Case No. S19A0769

COALITION FOR GOOD GOVERNANCE,
RHONDA J. MARTIN, SMYTHE DUVAL, and JEANNE DUFORT,

Plaintiff-Appellants,

v.

BRAD RAFFENSPERGER, *Secretary of State*, FULTON COUNTY BOARD OF REGISTRATION AND ELECTIONS, GWINNETT COUNTY BOARD OF REGISTRATIONS AND ELECTIONS, and GEOFF DUNCAN

Defendant-Appellees.

BRIEF OF ELECTION SECURITY EXPERTS and NATIONAL ELECTION DEFENSE COALITION AS AMICI CURIAE IN SUPPORT OF PLAINTIFF-APPELLANTS

Fulton County Superior Court
Case No. 2018CV313418

Russell T. Abney, Georgia Bar No. 000875
Blake Tanase, Georgia Bar No. 544067
FERRER, POIROT & WANSBROUGH
2100 RiverEdge Parkway
Sandy Springs, Georgia 30328
(800) 661-8210

Pro Bono Counsel for Amici Curiae

STATEMENT OF INTEREST

Amici curiae are nationally recognized experts in election security and the nonpartisan, nonprofit organization, the National Election Defense Coalition (NEDC). The NEDC is a national network of recognized experts in cybersecurity and elections administration, bipartisan policymakers, and concerned citizens who seek to assure that all elections are conducted with appropriate cybersecurity protections and use election technologies that accurately report and tabulate the voters' choices. *Amici* include the following individuals with expertise in the security of electronic voting systems.[1]

Prof. Duncan A. Buell is the NCR Professor of Computer Science and Engineering at the University of South Carolina. Professor Buell has published peer-reviewed research papers on voting technology security, with particular attention to security vulnerabilities and methods for verifying tabulation accuracy. After earning a Ph.D. in mathematics in 1976 from the University of Illinois at Chicago, and an award of tenure in the Department of Computer Science at Louisiana State University, he worked for 15 years at the Institute for Defense Analyses (IDA). IDA is a computing research laboratory that supports the National Security Agency in protecting the nation from hostile foreign adversaries and an

[1] Institutional affiliations are provided for identification purposes only. These affiliations do not constitute or reflect institutional endorsement of this briefing.

array of threats. Upon return to academia, Professor Buell chaired the Department of Computer Science and Engineering at the University of South Carolina from 2000 through 2009 and served as interim dean of his college during 2005-06. Professor Buell began working on voting systems security and accountability with the League of Women Voters of South Carolina in 2004. Professor Buell has served as a consulting voting systems security expert on technical anomalies arising in numerous jurisdictions nationwide.

Candice Hoke is the Founding Co-Director of the Center for Cybersecurity and Privacy Protection and a law professor emerita at Cleveland State University. She holds a M.S. in Information Security from Carnegie Mellon University, and a J.D. from Yale Law School. She served as a research Team Leader for the California Secretary of State’s pathbreaking study of voting system security (TTBR, 2007), and a member of the Cuyahoga Election Review Panel (2006) that examined the causes for major election failure that included myriad failures of technical election equipment. She served on the American Bar Association’s (ABA) Advisory Commission to the Standing Committee on Election Law (2007-10), and co-authored a guide for election officials and their lawyers on when to convene a forensic evaluation. She has published numerous articles and book chapters on election cybersecurity issues, and the legal frameworks for protecting voting rights despite the use of flawed technologies. She has provided consultation on election security issues for high level personnel from the U.S. Departments of Homeland Security, Defense, and Justice, from 2008-17, and testified before Congress on election auditing as a component for assuring public trust in the election system. She was a *Yale Law Journal* editor, a judicial clerk for the U.S. Court of Appeals for the First Circuit, and a litigator, before becoming a law professor and cybersecurity consultant.

David Jefferson, Ph.D., is a computer scientist working at the intersection of computing and public elections for over two decades. For much of his career, Dr. Jefferson worked on supercomputing applications for national security at Lawrence Livermore National Laboratory. He holds a PhD from Carnegie Mellon University, and formerly taught computer science at UCLA. At the request of five California Secretaries of State (SoS) and numerous election officials, he worked for two decades to improve California election security. Jefferson was appointed by Secretary of State Debra Bowen as chair of the Post-Election Audit Standards Working Group that worked parallel to the Top to Bottom Review study of California voting systems security. He also served as the chair of the SoS's Technical Advisory Board under Secretary Kevin Shelley, and then as chair of its successor Board under Secretary Bruce McPherson. In 1999, he led the technical side of an SoS task force in its study and report on Internet voting. He subsequently served on the National Science Foundation-Internet Policy Institute panel on

Internet voting, and testified to the National Commission on Federal Election Reform organized by presidents Carter and Ford. He has consulted with numerous agencies and States on the subject of voting security, including for the Federal Election Commission and the Department of Defense. He is also a co-author of the SERVE Security Report (servesecurityreport.org), which detailed the security vulnerabilities in the Defense Department's proposed Internet voting system in 2004. More recently, he has served as Chair of Verified Voting's Board of Directors and currently serves as a member of that Board.

Andrew W. Appel is the Eugene Higgins Professor of Computer Science at Princeton University. Professor Appel received his PhD in Computer Science from Carnegie Mellon University in 1985 and since 1986 has been on the faculty of Princeton University. He was elected a Fellow of the Association for Computing Machinery in 1998 and received the ACM SIGPLAN Distinguished Service Award in 2002. From 2009-2015 he served as Chair of the Department of Computer Science. He has published over 120 books and papers about programming languages, compilers, computer security, voting machines, program verification, and technology policy. He has performed two court-ordered forensic examinations of voting machines (and election-management computers) in different cases in New Jersey. He served on the National Academies of Science, Engineering, and

Medicine (NASEM) study committee that produced the 2018 report, *"Securing the Vote: Protecting American Democracy."*

Joseph R. Kiniry, Principal Scientist, Galois and Principled CEO and Chief Scientist, Free & Fair. Dr. Joseph Kiniry is a Principal Scientist at Galois and the Principled CEO and Chief Scientist of Free & Fair. He has been a tenured academic at four universities in three countries. His PhD is from the California Institute of Technology. He has nearly twenty years' experience in the design, development, support, auditing, and hacking of electronic voting systems and has served as an adviser to the US, Dutch, Irish, and Danish governments in matters relating to electronic voting.

David A. Bader is Professor and Chair of the School of Computational Science and Engineering, College of Computing, at the Georgia Institute of Technology. He is a Fellow of the IEEE and AAAS and advises the White House, most recently on the National Strategic Computing Initiative (NSCI). Dr. Bader is a leading expert in solving global grand challenges in science, engineering, computing, and data science. His interests are at the intersection of high-performance computing and real-world applications, including cybersecurity, massive-scale analytics, and computational genomics, and he has co-authored over 230 articles in peer-reviewed journals and conferences.

Dr. Mustaque Ahamad is a professor of computer science at the Georgia Institute of Technology. He also serves as chief scientist of Pindrop Security, which he co-founded in 2011. Dr. Ahamad served as director of the Georgia Tech Information Security Center (GTISC) from 2004-2012. As director of GTISC, he helped develop several major research thrusts in areas that include security of converged communication networks, identity and access management and security of healthcare information technology. Dr. Ahamad received his Ph.D. in computer science from the State University of New York at Stony Brook in 1985. He received his undergraduate degree in electrical and electronics engineering from the Birla Institute of Technology and Science, Pilani, India.

SUMMARY OF ARGUMENT

Computers automate and increase the efficiency of many governmental and business functions, but they are not infallible, as complex litigation concerning electronically stored information frequently exposes. Numerous financial, medical, and other institutions have discovered that their computers too often present erroneous data as if it were correct. Sometimes these errors are attributable to software bugs, other times to human input errors, and yet others are traceable to hacking or malware. The integrity of the data within such computer or information systems is also vulnerable to degradation from a wide variety of potential causes. Hence, in both routine operations and complex litigation, institutions deploy third-party forensic investigation firms (and sometimes their own expert staff having technical forensic and IT auditing skillsets) to assess the causes of anomalous computer conduct, enable data correction, and mitigate the likelihood that these performance problems will repeat. Forensic activities in these contexts are expected as a part of sound business judgment and due diligence, and in the discovery process provide the basis for a trial court or jury to make sound findings of fact. The use of computer scientists and cybersecurity experts is anticipated and relied on by trial courts for forensic investigation of electronic records in commercial litigation when seeking to determine the cause or extent of issues in controversy for judicial adjudication.

Election system computers should be understood and managed in similar ways to those containing banking and medical records. If, during an election, election computers have produced indicators of malfunctioning in ways that might affect their data accuracy and integrity—most importantly, the accuracy of the vote records and tabulations—qualified forensic investigation must ensue, particularly in the proceedings of an election contest.

While finality in the outcomes of elections is important, that finality must be founded on a fair process and factual accuracy. When sufficiently severe computer data anomalies are documented, as they were in Georgia's 2018 Lieutenant Governor election, sound judgment counsels a forensic investigation to ascertain what the causes of the anomalies were and whether they impacted the accuracy of reported vote totals (as the statistical analysis suggested had occurred). A properly-constructed forensic evaluation, considered by a trial court, supports public respect for the election officials and the system. Such a process demonstrates the good-faith efforts of the courts in safeguarding the election and voting rights. Computers are fallible. For a computer-based voting system to be legitimate, there must be meaningful accountability checks and quality assurance processes. Such is the case for any other piece of equipment whose dysfunction can cause harm.

Recognizing the value of this level of election transparency to the public interests, some jurisdictions make their election management system databases (such as the GEMS database) a matter of ***public*** record. For example, after a four-day trial and an *in camera* review of the database, the Pima County, Arizona Superior Court determined that permitting the public to conduct *its own* examinations of the GEMS database was in the public interest, declaring them to be public records. Conversely, if after significant indicators of computer malfunctions, courts permit election officials to block electronic election data from electors who challenge an election, essential questions will go unanswered and voter confidence will quickly erode.

This election contest at issue merits expert examination of the electronic records in the context of the anomalous results and other alleged irregularities. The trial court's order dismissing the Plaintiffs' complaint should be reversed, and the case remanded for adequate electronic records discovery.

<u>Argument</u>

A. Substantial Evidence of Serious Computer-Based Anomalies Warrants a Forensic Investigation into Election Computers and Databases

The myriad election computer malfunctions and aberrational statistical evidence that Plaintiffs have adduced cannot be investigated or explained without a forensic examination of the electronic records of the computers involved in the 2018 election process. Without a forensic assessment, the causes of the anomalies remain unknown and unexplained—which means that the factual bases for determining whether legal rights have been infringed upon and relief should be granted will remain concealed.

Preventing forensic investigation not only blocks potential vindication of important legal rights, but also implicitly encourages covert tampering with election computers and tabulations, as courts would be shielding such tampering from discovery. The nature of software-based voting machines permits covert election cheating. Unless the courts exercise sufficient oversight via the discovery process, malefactors may view Georgia's election computers as offering "open season" for tampering.

Whether attributable to software programming bugs, deliberate intrusions by human operators, or other reasons, Georgia's election computers may have suffered "incidents" or "events" that can be uncovered and explained only pursuant to qualified forensic analysis and explained. Plaintiffs' Diebold voting system expert Matthew Bernhard opined that "[t]he errors reported during the November 2018 election, particularly in the Lieutenant Governor's race, are consistent with a pattern of either malicious tampering, software error, or incorrect programming of the election." (R. 1001 ¶31).

More specifically, the wide range of computer performance anomalies and statistical aberrations gathered thus far preceding discovery include:

1. The significant drop-off in recorded votes ("undervote") in the Lt. Governor's race versus other races further down the ballot; estimated at 127,000 votes. (R. 985 Conclusion). Professor Philip Stark emphasizes that the undervote rate differed substantially by the type of ballot cast—electronic or paper. The undervote rate was "substantially higher for ballots cast on direct-recording electronic (DRE) equipment than for ballots cast by mail using paper ballots, by an amount that cannot reasonably be ascribed to chance." (R. 513 ¶22).
2. Some voters reported that because of the touchscreen machine's failure to display the Lt. Governor's race, they were unable to vote for Lt. Governor candidates on the electronic ballot on DRE machines until they reached the final touchscreen summary/verification screen. Only by scrolling back through the ballot could did

the machine to display the Lt. Governor race for voting. (R. 40 ¶40, 42 ¶43, 1729).

3. Some DRE touchscreen machines automatically cast the electronic ballot from the review screen before the voter was permitted time to review and confirm their choices. (R. 41 ¶41).
4. Some DRE touchscreen machine(s) displays failed to show a valid candidate's name, and assigned the wrong party to another. (R. 42 ¶42).
5. A number of DRE touchscreen machines cancelled voters' ballots while voter was in the process of selecting candidates and marking the electronic ballot. (R. 42 ¶R 43).
6. Some voters reported DRE touchscreen machines demonstrating "vote flipping," which is when the voter presses the target area "button" for one candidate, but the machine registers a vote for a different candidate. (R. 43 ¶45, 44 ¶47).
7. Some precincts showed discrepancies between the public count of voters and the total number of ballots cast that were reported on the DRE touchscreen machine tapes (at the closing of the polls). (R. 43 ¶46).
8. Discrepancies identified between DRE poll tape precinct totals and precinct results reported by the GEMS system in some polling places. (R. 44 ¶46, ¶48).
9. In a number of African American neighborhood precincts, a statistically significant, unexpected, and apparently unprecedented greater drop-off

(undervote) occurred in the Lt. Governor's race as compared with the Governor's race.[2]

10. Individual touchscreen machines which reported significantly different results patterns than the other machines in the precinct, such as one machine showing significant winning margins for one party when all other machines in the precinct showed significant margins for the opposing party. (R. 514 ¶ 24-30).

11. Errors in the electronic pollbooks used to authenticate and check-in voters so they can vote; potentially (and reportedly) caused by unauthorized changes in the voter registration records, possibly a result of a compromised or malfunctioning voter registration database. (R. 21 ¶ 2).

B. The Forensic Assessments that Plaintiffs Seek for Georgia Election Computers and Databases are Common Techniques in Other Litigation and Should Be Authorized Here.

Defendants seek to block the types of digital evidence collection, examination, and analysis that, in other sectors, are commonly a part of due diligence and routine discovery in litigation. Given the threat of covert cyberattacks that can change the election outcomes from the choices Georgia's

[2] *See Fair Fight Action et al v Raffensperger* (N.D.Ga.18-cv-05391) [Doc. 41 ¶ 105] (" Indeed, recent analysis of the results of the Lieutenant Governor's race in the 2018 Election shows a statistically unexpected drop-off in the number of votes compared to the number of votes cast in the Governor's race. That drop-off was significantly more pronounced in primarily African American precincts than it was in non-minority precincts."). *See also* Michael Harriot, *Thousands of Black Votes in Georgia Disappeared and No One Can Explain It*, THE ROOT, Feb. 9, (2019), available at: https://www.theroot.com/exclusive-thousands-of-black-votes-in-georgia-disappea-1832472558 (last visited May 2, 2019).

voters had made, the scientific literature that documents the ease of tampering with the GEMS vote tabulation database in largely undetectable ways, Georgia election officials may not have defended against or detected such incursions. A forensic inquiry is thus appropriate.

Printed standard reports from the election management system (in this case, the Diebold GEMS system) would not inform an examiner of a programming, configuration, or operational error, and would not reveal malicious hacking or the scope of such irregularities. As Professor Philip Stark noted in his affidavit, the "investigation most likely to produce definitive evidence is a forensic examination of the hardware and software of DREs and other computerized systems used by Georgia." (R. 517 ¶32).

Plaintiffs' voting system expert Matthew Bernhard correctly states in his affidavit that "the only way to determine the extent and number of votes potentially impacted by programming errors or malfunctions is to review the electronic programming and operating files used during the election. No standard report that is printed by the Diebold system would expose a programming error, in particular because the programming that generates such reports may itself be faulty. Only a review of the electronic files containing the programming would detect errors." (R. 904 ¶ 10).

C. Discovery of the GEMS Databases is Appropriate and Would Not Negatively Impact Election Security but Instead Would Promote Election Security via Accountability and Transparency

1. Analysis of the GEMS Database is an efficient first step to locate coding errors

GEMS is the election management system utilized by the Diebold DRE voting system used by the State of Georgia. An election management system is a “set of processing functions and databases within a voting system that defines, develops and maintains election databases, performs election definitions and setup functions, format ballots, count votes, consolidates and report results, and maintains audit trails.”[3] The GEMS database is built in Microsoft Access, and contains the ballot and machine configuration instructions in a worksheet format that can be efficiently analyzed. Diebold voting system experts are aware that the GEMS database “fails to conform to fundamental database design principles and software industry standards for ensuring accurate data. Thus, in election tabulations, aspects of the GEMS design can lead to, or fail to protect against, erroneous reporting of election results.” [4] Therefore, the potential corruption of the GEMS database requires a thorough examination of the details and configuration of the database

[3] U.S. Election Assistance Commission – Version 1.0 Volume I: Voting System Performance Guidelines, Appendix A: Glossary A-10.

[4] *See* Thomas P. Ryan and Candice Hoke, *GEMS Tabulation Database Design Issues in Relation to Voting Systems Certification Standards*, *in* 2007 Usenix/Accurate Electronic Voting Technology Workshop, *available at* https://www.usenix.org/legacy/events/evt07/tech/full_papers/ryan/ryan.pdf

itself when there are indications of potential errors in reported results. No standard report produced or display of archived files on the DRE touchscreen will detect the source of the errors.

In order to investigate and potentially discover the cause of certain election irregularities such as an anomalous undervote rate, one should first examine the GEMS database, in its human readable Microsoft Access format. An examination of GEMS database may, for example, reveal quickly that the database was coded to record votes case for Candidate A as votes cast for Candidate B, or that votes cast for Lt. Governor were actually being recorded as votes for State Senate District 47 candidates, or that some ballot styles displayed on the touchscreen erroneously failed to include a given contest. The examination could also reveal some signs of tampering.

It is notable that the Secretary of State's office, after receiving a formal complaint about the significant undervote rate and a request for investigation (R. 66-68), undertook no such review to determine if the GEMS database had a configuration error or other easily identifiable discrepancy (according to the representative's testimony). (T-385:11-14). Such an examination is now imperative in discovery for the trial court to be informed as to whether identifiable errors are present that could have had material erroneous impact on the election outcome.

2. GEMS database examination by experts is not a material security risk

The Pima County, Arizona State Superior Court's 2007 decision regarding the public nature of the Arizona's GEMS databases explains the operation and importance of the database in analyzing the election results. *Democratic Party of Arizona v. Pima County Board of Supervisors* (Ariz. Sup. Ct. 2007) (Case No. 20072073) (attached as Exhibit A). Before declaring the final copy of the GEMS database to be a public record, the Arizona state court gained an understanding of its contents in an *in camera* review and in a four day trial to consider the balancing of security and election transparency interests. *Id.* at 1. Any examination of the GEMS database in discovery in this case could have been covered by experts' confidentiality agreements, and not be deemed a public record, it should be noted that the Arizona court ordered *public* disclosure of GEMS databases.

The description of the operations of the GEMS database in the Arizona court's ruling (*Id.* at ¶¶ 5-21) appears consistent with the standard manner in which GEMS works. It is clear that the GEMS database contains human readable election data, not proprietary source code. The usefulness of the GEMS database is well articulated, as is the low risk of increasing security vulnerabilities.

The court's ruling notes that Alaska also disclosed its GEMS database without negative consequences. *Id.* at ¶ 33. There are no known negative security consequences of the Arizona databases being disclosed as public record after the

Arizona court's ruling. Marin County, California's June 2010 election GEMS database is posted on the internet.[5] Likewise, there are no known negative security consequences of publicly releasing the Marin County database or any other GEMS post-election databases.

It is unlikely that disclosure of the GEMS database to experts for examination under confidentiality agreements poses a meaningful security risk to Georgia's elections. Yet the benefits of expert review are clear and such an examination is essential to gain an understanding of what factors generated the anomalous results in Georgia's Lieutenant Governor's race, and the cause of the other widespread alleged voting system irregularities required to present the needed evidence to the trial court.

3. Standard GEMS reports cannot substitute for a forensic examination

The standard public record reports from the GEMS election management system offered by the Defendants and ordered by the trial court for discovery (Base Precincts With Races Report, Ballot Image Report, Vote Center With Cards Report, Statement of Votes Cast Report, and Summary Report) may be useful to assist the experts in targeting specific machines or precincts for

[5] Indeed, the data can be downloaded at the following web address: http://blackboxvoting.org/docs/diebold/june10-primaryFINAL.zip

forensic examination and determining priorities for the examination, but cannot be substituted for an examination of the database itself.

While the data from the Ballot Image Reports (a representation of the votes recorded for each individual ballot) could have been useful in further targeting priorities for forensic examination, the number and format of the reports would have made the examination logistics virtually impossible. Over 400,000 reports would have been generated by Fulton County alone,[6] in a format that would require time-consuming processing by third party applications to convert into a usable database—information that would have been simple to analyze in the GEMS MSAccess database. However, it appears that these hundreds of thousands of ballot image reports ordered by the court were not produced to the Plaintiffs,[7] preventing even a cursory analysis by the Plaintiffs' experts.

4. Internal memory of the voting machines requires forensic analysis

Whether or not defects are found in the GEMS database, a sample of touchscreen DREs' internal memories should be examined to confirm the transfer of defects located in the GEMS database and inspect for additional defects or signs of system malfunction. The Georgia election code requires the

[6] Supplemental Brief of Appellants, April 30, 2019, at 6.
[7] *Id*.

internal memory of machines be maintained during the period of a potential or existing election contest, anticipating that the examination of the DREs' internal memory may be required in an election contest.[8]

The trial court ordered that confidentiality agreements be executed to protect any confidential information[9]. This is a customary and generally accepted approach for protecting any sensitive information that may reside in the electronic records while they are being examined by experts. The potential that sensitive security-related information could exist in the internal memory or GEMS database should not preclude the experts' examination protected by a non-disclosure agreement. Given the types of anomalies and irregularities alleged in this case, a review of the internal memory of machines selected by Plaintiffs' voting system experts is needed to determine the source and potential impact of the problems.

[8] Georgia Election Code 183-1-12-.02(6)(d) reads:

> The election results, ballot styles, ballot images, and other information for each election stored in the internal memory storage of each DRE unit shall be maintained for a minimum of one month following each election after which time the results may be erased provided that there are no election contests pending concerning such election."

It is imperative that custodians of the DRE machines comply with this provision's mandate to preserve the internal memory while the election tabulation may be subject to controversy. Preservation of the memory is essential because there is no independent record of the voters' votes to audit in order to settle a dispute. The instructions and data resident in the internal memory can offer evidence of tampering, erroneous coding or machine malfunction. However, every post-election use and operation of the machine weakens and alters the electronic record in the internal memory for purposes of a proper forensic examination to determine the potential cause of the anomalous result. Matthew Bernhard's affidavit describes the nature of the internal memory of the Diebold DRE. (R. 990-998).

[9] January 11, 2019 Order on Discovery at 6.

From the parties' briefs, it appears the trial court ordered an examination of the internal memories of some voting machines, selected not by the Plaintiffs' experts, but by the trial court. (R. 879 ¶2). It appears, however, that the Plaintiffs were offered only the opportunity to review voting machine video displays of archived reports from the disputed election. (R. 896-897). Such displays of reports are not the "internal memory" of the voting machine and are not an adequate substitute for a review of the internal memory. Voting system and forensic experts would be unable to draw any meaningful conclusions to present as credible evidence to the trial court from simply a review of archived results reports on touchscreen video displays. Further, mindful of the provisions of Georgia Election Code 183-1-12-.02(6)(d), examination of DRE machines' memory cards archived data on a DRE machine will alter the internal memory, weakening its forensic value. Plaintiffs experts were operating under established best practices when they insisted that back-up copies of the internal memory be made by Defendants before examining the machines.

Voting system experts would most likely require multiple weeks of forensic examination of the internal memories of a carefully selected sample of DRE machines used in the election in controversy to issue reports on which the trial court could rely for accurate findings of fact.

CONCLUSION

According to the case record, the Plaintiffs' statistical expert, Diebold voting system expert, and election data expert agree: the significant size of the undervote in the Lieutenant Governor's election that occurred in votes cast on DREs but not on paper ballots strongly suggests that malfunction, misconfiguration, bugs, hacking, and/or other error or malfeasance caused some DREs not to properly record votes in the Lt. Governor's contest. An expert examination of the electronic election configuration files and records residing in the GEMS database and the DRE internal memory is required to determine the cause of the potential defects and the estimated impact. The GEMS results reports ordered produced by the trial court and the review of archived election files displayed on DRE screens are woefully insufficient by any standards for the detection, analysis, and confirmation of the defects that may have caused the irregularities and anomalous undervote rates in the Lieutenant Governor's race.

For these reasons, the trial court's order dismissing the Plaintiffs' complaint should be reversed, and the case remanded for adequate electronic records discovery.

Respectfully submitted this 3rd day of May, 2019.

/s/ Russell T. Abney
Russell T. Abney
Georgia Bar No. 000875
Blake Tanase

Georgia Bar No. 544067
FERRER, POIROT & WANSBROUGH
2100 RiverEdge Parkway
Sandy Springs, Georgia 30328
(800) 661-8210
rabney@lawyerworks.com
btanase@lawyerworks.com

Pro Bono Counsel for Amici Curiae

CERTIFICATE OF SERVICE

I hereby certify that, on this date, I served the foregoing **Brief of Election Security Experts and National Election Defense Coalition as Amici Curiae in Support of Plaintiff-Appellants** upon all parties of record through their counsel.

This 3rd day of May, 2019.

/s/ Russell T. Abney
Russell T. Abney
Georgia Bar No. 000875

EXHIBIT A

ARIZONA SUPERIOR COURT, PIMA COUNTY

JUDGE: HON. MICHAEL MILLER CASE NO. 20072073

COURT REPORTER: NONE DATE: December 18, 2007

DEMOCRATIC PARTY OF PIMA COUNTY,
Plaintiff,

v.

PIMA COUNTY BOARD OF SUPERVISORS, a
body politic,
Defendant.

UNDER ADVISEMENT RULING

Plaintiff Democratic Party of Pima County brings this statutory special action to compel Defendant Pima County Board of Supervisors ("Pima County") to disclose "every file stored in the Pima County's election computer that ends with the extension "gbf" or "mdb," and the password for "gbf" files." Pima County refused the request on the basis that A.R.S. § 16-445(D) prohibits their disclosure and, in any event, the government interest in secure elections outweighs Plaintiff's interest in the files. The Court conducted a four day trial beginning December 4, 2007 to address the statutory and balancing arguments. The Court also inspected *in camera* on a secure laptop computer the 2006 General Election mdb file using GEMS and Microsoft Access.

This Ruling provides the Court's findings of fact and conclusions of law.

Lynne Booth
Judicial Administrative Assistant

RULING

Findings of Fact and Conclusions of Law

1. Plaintiff Democratic Party of Pima County is a political organization recognized by statute. *See* A.R.S. §§ 16-801 to 16-828. The organization includes county representatives selected pursuant to A.R.S. § 16-821. As a political party, Plaintiff is authorized to participate in the accounting and monitoring of elections. *See* A.R.S. §§ 16-602 and 16-603. Plaintiff actively exercises its right to monitor elections and it has offered a variety of recommendations to improve the integrity, transparency, and security of elections in Pima County. The records request for the election computer files arises out of its statutorily-mandated role.

2. Defendant Pima County Board of Supervisors is a body politic. Pursuant to its own regulations, day-to-day functioning is delegated to County employees. *See* Pima County Code 2.12.090. Individual supervisors are prohibited from making or interfering with the functions and decisions of County employees. *Id.* The County Administrator, Charles Huckelberry, has final authority to make individual decisions on specific record requests, such as the request made by Plaintiff. Mr. Huckelberry makes those decisions in consultation with technical advisors and with the advice of counsel.

3. The Pima County Division of Elections is charged with the responsibility of conducting most elections in Pima County. The division head is Brad Nelson. Mr. Nelson is responsible for conducting elections pursuant to state and federal law, organizing the necessary personnel and

equipment to conduct the election and tally the votes, and planning for secure but transparent elections. Mr. Nelson answers directly to Mr. Huckelberry.

4. On December 6, 2006 Plaintiff made a written, ten-item records request to Mr. Nelson and the Board chairman. Only the first item is at issue. The requested files are described as follows:

> Electronic copies of the Diebold GEMS database for both the primary and general election and backup (if present) Diebold "Central Tabulator" computers. These should be produced on a CD or portable disc drive in the presence of Democratic Party observers and under their supervision. We can bring a blank factory-sealed 100 gig or more USB hard disc for simple transfer of these records.

On January 8, 2007 Mr. Huckelberry informed the Board of Supervisors in a memorandum that the request had been denied:

> The County has responded to the public records request of Mr. Risner (attached) regarding Elections information. Item 1 of the request will not be provided. It is the consensus of technical opinion that providing a copy of the electronic database used to tabulate primary and general election results is ill-advised and would provide, to a knowledgeable individual, an appropriate roadmap to hack a future election in Pima County. In consultation with the Secretary of State's Office and the Maricopa County Attorney's Office, it was determined to be inappropriate to release the database. Hence, it will not be provided to Mr. Risner.

In response to the denial and intervening events, Plaintiff enlarged its request from computer files for the 2006 elections to "include every file that ends with the extension "gbf" or "mdb" . . . this request is not limited to the dates originally requested and does include all those files stored on the computer." On March 30, 2007 Deputy County Attorney Karen Friar wrote to Plaintiff's counsel to inform him that

"After much deliberation, Pima County has determined that it cannot honor the public records request would indeed be detrimental to the interest of the government in providing for a secure and honest election." Following the denial, Plaintiff filed this statutory special action pursuant to A.R.S. § 39-121.

Elections Computer System

5. The Pima County Division of Elections uses Diebold System Inc.'s Global Election Management System ("GEMS") to process elections. GEMS has been certified by the Arizona Secretary of State for use in Arizona. The parties agree that the GEMS program is not subject to disclosure.

6. The GEMS program has several primary functions. First, it is used to print the ballots. This is a more complicated process than first appears because most general elections have races that do not apply to all county voters. Additionally, ballots are rotated from precinct to precinct. There can be as many as sixteen hundred ballot styles.

Second, GEMS writes the memory cards used to program optical ballot scanners and touch screen displays (hereinafter "voting machines"). These memory cards are integral parts of a ballot scanning process.

Third, GEMS tallies the votes from the voting machines. This process involves processing many different digital inputs, sometimes on a concurrent basis.

Finally, GEMS prints a variety of reports from the race results to management and audit functions.

Lynne Booth
Judicial Administrative Assistant

7. GEMS is a stand-alone program designed to run on computers with a Microsoft Windows operating system. The current version used by Pima County is 1.18.24.0. The GEMS software is an executable file. The program is derived from human-readable source code that is then compiled into object (machine-readable) code. The source code is copyrighted and only available through a license agreement with the manufacturer. A copy of the source code is held in escrow with the Arizona Secretary of State.

8. GEMS creates a relational database. The database consists of tables of information (*e.g.*, race, candidate, precinct) and queries (pre-formed requests for particular information).

9. GEMS creates one database file for each election. The format is based on the format used by Microsoft Access, a general database program. Each database file ends with the letters "mdb," which stands for "Microsoft DataBase." The filename extension nomenclature follows a system used with other applications in the Microsoft Office Suite, such as Microsoft Word (.doc), Microsoft Excel (.xls), and Microsoft Powerpoint (.ppt). That is, the application creates a file with a specific three-letter extension to identify its relationship to that application.

10. A "gbf" file is a password-protected, compressed, and encrypted version of the mdb file. A gbf file can only be created and opened by the GEMS program. For the purpose of this case, the distinctions between a gbf and mbd file are irrelevant. The remainder of the Order refers only to the mdb file, although it applies equally to the gbf counterpart.

Lynne Booth
Judicial Administrative Assistant

RULING

11. The GEMS-created mdb file can be opened using Microsoft Access. Data in the file can be manipulated. Password protection can be overwritten. The full functionality of the GEMS program, however, cannot be utilized if the mdb file is opened in Microsoft Access. GEMS is necessary to utilize all of the election-related functions.

12. Although the Microsoft-sponsored mdb format is widely used, it has size and input limitations. Specifically, file integrity becomes less robust (*i.e.*, prone to crashing) when the database becomes too large. The data may also become corrupted if it receives too many inputs, too quickly, at one time (concurrency problems). These limitations are well known. Microsoft has warned against using the mdb format for some critical applications, such as election management software.

13. The parties agree that "[t]here are significant security flaws with the architecture of the GEMS software." Each of the expert witnesses endorsed that statement to one degree or another.

Is An MDB File A "Computer Program?"

14. A.R.S. § 16-445 requires Pima County to file with the Secretary of State "a copy of each computer program for each election." The filing must be made at least ten days before the election. Any revisions to the computer program must be filed within 48 hours after the revision. A.R.S. § 16-445(B).

Electronic medium used to operate the vote tabulating devices must be kept under lock and seal. A.R.S. § 16-445(C). If there is a retally of the votes, the election officer must submit an affidavit vouching for the authenticity of the electronic medium and that there has been no alteration since the election. *Id.* There is no requirement that the mdb file be sent to the Secretary of State after the election. *See generally* Arizona Secretary of State Election Procedures Manual, pgs. 79-80 (Aug. 2006).

Pima County argues that A.R.S. § 16-445(D) prohibits disclosure under the public records law. It provides that "[a]ll materials submitted to the secretary of state shall be used by the secretary of state or attorney general to preclude fraud or any unlawful act under the laws of this title and title 19 and shall not be disclosed or used for any other purpose." The issue is whether a "computer program" ordered to be filed with the Secretary ten days before the election includes the mdb file created by GEMS during the election process, but which is not finalized until after the votes are counted.

15. "Computer program" is described as "all programs and documentation adequate to process the ballots at an equivalent counting center." A.R.S. § 16-444(A)(4). "Database" is not defined in the election statutes or other Arizona law.

16. Federal copyright law defines "computer program" as "a set of statements or instructions to be used directly or indirectly in a computer in order to bring about a certain result." 17 USCA § 101. Even such a simple definition made within the context of a specialized area of law is subject to problems of context and nuance. *See* William F. Patry, *Copyright and Computer Programs: It's All In The Definition*, 14 Cardoza Arts & Ent. L.J., 1, 39 (1996). Nonetheless, there is a fundamental distinction between a computer program and a database. *Compare* Copyright Office Circular 61 *Copyright Registration for Computer Programs* (a "computer program" is a set of statements or instructions to be

used directly or indirectly in a computer in order to bring about a certain result") with Circular 65 *Copyright Registration for Automated Databases* ("database is a body of facts, data, or other information assembled into an organized format suitable for use in a computer and comprising one or more files").[1]

17. The expert witnesses also agreed that an mdb file is fundamentally different from the GEMS executable file. The latter is not readable by a human. It contains the majority of the instructions to operate the computer. The only disagreement is whether the addition of queries, which are in the form of "SQL" statements, transform the mdb file into a computer program.

18. The Arizona Secretary of State creates and distributes the Elections Procedures Manual that provides additional details to election officials regarding the conduct of elections and the filing of mandated materials. The Elections Procedures Manual does not provide explicit instruction on whether the mdb file may be disclosed. Gila County Election Director, Dixie Mundy, testified that the Secretary of State provides training materials and seminars. She does not recall any instruction from the Secretary of State prohibiting the disclosure of mdb files. Finally, the Secretary of State's Election Director, Joseph Kanefield, testified pursuant to a Rule 30(b)(6) designation about the Secretary's policies and procedures regarding election software. He did not indicate that the Secretary of State opines that A.R.S. § 16-445 prohibits disclosure. Similarly, the Arizona Attorney General, which represented the Secretary

[1] Copyright protection specifically extends to "computer programs" whereas databases may be copyrightable as a form of original compilation. *Id.* The point is not whether GEMS versus the mdb file is subject to copyright; rather, the importance lies in the recognized legal distinction between the software program that creates a database and the database itself.

of State in this case and conducted an investigation relating to the computer files, did not seek intervention in this case to oppose disclosure of the mdb files.

19. The final mdb files (which are the principal files requested by the Plaintiff), are not required to be sent to the Secretary of State. Unofficial results that are released to the public must be transmitted to the Secretary by telephone, fax, or "other electronic means." A.R.S. § 16-622(B). The official canvas for all elections must be provided to the Secretary "on paper and also electronically in a 'readable' format prescribed by the secretary of state." Elections Procedures Manual at 158 (2006); *see also* A.R.S. §§ 16-646(B) and (C). Nothing in the vote tallying statutes or the Elections Procedures Manual indicates that Pima County is required to provide to the Secretary the final mdb file.

20. The Court finds that the mdb file is not a computer program as defined under A.R.S. § 16-444(A)(4) for three reasons. First, the legal distinction between a computer program and database is well recognized in other contexts and applies equally here. *See e.g.,* Raymond T. Nimmer, 1 Information Law § 3:33 (2007); Amy Sullivan, *When The Creative Is The Enemy Of The True: Database Protection In The U.S. And Abroad*, 29 AIPLA Quarterly J. 317, 323 (2001). Second, computer experts recognize the distinction between a computer program and a database. Finally, the prohibition against disclosure, when read in the context of all elections statutes, does not include the final mdb files because they are not required to be provided to the Secretary in that form.

21. The Court concludes that A.R.S. § 16-445(D) does not prohibit disclosure of mdb files.

Lynne Booth
Judicial Administrative Assistant

Balancing Plaintiff's Right To Public Records Versus Defendant's Interest In Conducting Secure Elections.

22. The parties agree the mdb files are public records.

23. The public records law creates a strong presumption in favor of disclosure. *Griffis v. Pinal County*, 215 Ariz. 1, 4, ¶¶ 12-13, 156 P.3d 418 (2007). If a public record falls within the scope of the statute, the Court can perform a balancing test to determine whether privacy, confidentiality, or the best interests of the state outweigh the policy in favor of disclosure. *Id.; see also Carlson v. Pima County,* 141 Ariz. 487, 490-491, 687 P.2d 1242 (1984).[2]

24. Pima County is concerned that each of the primary functions of the GEMS software could be compromised if the database is released to Plaintiff. The concerns are based on several assumptions, which the Democratic Party does not deny. First, release of the computer file to Plaintiff will likely result in wide disclosure. Second, although Plaintiff does not seek disclosure of the GEMS software, the program is available on the Internet; persons who have not obtained an official license to operate the program can download it. The Court finds that disclosure of the mdb files will not be limited to Plaintiff.

[2] The balancing test generally focuses on "the public's right to openness in government" rather than the specific interest of the petitioner in the requested records. *Carlson v. Pima County*, *supra,* 141 Ariz. at 491. Although Plaintiff stresses its particular standing as a political party with specific rights and responsibilities in the elections process, the Court applies the *Carlson* standard.

Lynne Booth
Judicial Administrative Assistant

25. Pima County identifies four types of security compromises that could occur if the mdb files were released and there were lapses in physical security:

a. Counterfeit ballots could be generated from GEMS.

b. Counterfeit memory cards could be generated from GEMS.

c. Electronic transfer information could be obtained from the mdb file to launch a "man-in-the-middle" attack during transmittal of election results.

d. Counterfeit election results could be generated to confuse or call into question official election results.

26. Each of the concerns raised by Pima County represents a valid, significant security risk if physical security of the cast ballots, voting machines, memory cards, electronic input devices, and counting computer is not strictly maintained. For instance, the substitution of ballots or memory cards would require a lapse in existing security measures or the complicity of elections personnel to overcome lock-boxes and anti-tamper seals. Pima County acknowledges that its security measures would generally prevent insertion of counterfeit materials, but it wishes to maintain an additional layer of security in the event that those measures are not effective or are breached.

27. Interception of electronic transmissions and substitution of invalid voter results is an on-going concern. Specifically, the extant procedures involve modem transmission of voting machine results to the central counting computer. Interception of the electronic transmission would be made

easier if the transmission information contained within the mdb file was widely known. This is known as the "man-in-the-middle" ruse. There is a pending recommendation from Mr. Huckelberry to eliminate all modem transmission of voting machine results and to use a hardwire method within a secure-room environment. If Mr. Huckelberry's recommendation is accepted, the interception and substitution of voting machine results by remote electronic means is virtually eliminated.

28. The risk of interference with the counting computer has been significantly reduced by recent measures to control and monitor persons with access to the computer, to eliminate remote connections, and to create a special room that allows physical monitoring of the security measures. As with the counterfeit materials, it would be very unlikely that a contaminated mdb file could be substituted for the valid, working mdb file.

29. Use of the mdb file from past elections to create false election results in future elections does not appear to be a significant risk for several reasons. First, the printout of election results produced by GEMS has no security artwork (unlike the "timing marks" on ballots) and could be easily duplicated with any word processor. This possibility exists independent of disclosure of the mdb file. Second, persons not designated as elections personnel could not credibly claim that the election results they proffer are more valid than the results prepared from the secure, elections computer. Moreover, even such an attempt would likely result in a criminal investigation regarding fraud. *See* A.R.S. §§ 16-1012 to 16-1021 (penal provisions for interference, counterfeiting, intimidation, and corruption of the

Lynne Booth
Judicial Administrative Assistant

RULING

election process). Finally, Plaintiff concedes that the release of mdb files immediately after the polls close is neither practical or appropriate. Release of the mdb file days or even weeks after the election significantly reduces the concern that valid election results could be challenged with an altered mdb file.

30. Pima County also alleges that future mdb files would have to be "built from scratch" if past-election mdb files were released as public records. Bryan Crane, the master programmer for the Election Division since GEMS first came into use, explained how he builds the mdb file for each new election based upon prior files from previous elections. Use of prior mdb files is important because although the candidates and initiatives/referendums frequently change, the races and most precincts remain the same. Upon closer examination, however, his concern is a factual assumption for the more general concern about counterfeit ballots and memory cards.

Pima County's expert witness, Professor Merrill King, testified that starting over with a new mdb file for each election should not result in a new architectural structure for the mdb file or the formatting of ballots and memory cards. In fact, he emphasized that the primary risk of starting from scratch with each election is the increased likelihood of clerical errors because creating a ballot involves manual input of voluminous numerical and formatting data. Using the analogy of building a house, Professor King explained that the mdb structure for races and precincts (*i.e.,* equivalent to walls, number of rooms, etc.), must remain the same to comply with state and federal law, and only the contents (*i.e.,* furniture) must change to reflect the new candidates and questions. Using a prior, valid structure eliminates the likelihood of significant errors. The rationale for using prior mdb files as a template for future elections is valid and well-established.

Mr. Crane and Professor King suggested that by starting from scratch with each new election it would be possible to detect or prove counterfeit mdb files if public disclosure of the mdb file increased the risk that someone would do so to compromise an election. This potential problem ultimately returns to the concerns noted above regarding counterfeit ballots, memory cards, and substituted mdb files.

Plaintiff correctly points out that the risk of counterfeit items or reverse-engineering is primarily a concern if a perpetrator can physically substitute ballots, memory cards, or electronic transmissions with contaminated copies. These types of counterfeits are fundamentally different from counterfeiting in other areas where there is no attempt to eliminate or invalidate the real item (*e.g.*, counterfeit money, pirated DVD's, and unlicensed software have independent value separate from original items produced by the U.S. Treasury, movie companies, and software manufacturers).

31. In addition to the specific, identified concerns listed by Pima County, the witnesses also identified the threat of new attacks on electronic election systems that no one has anticipated. For instance, Plaintiff's expert, Mickey Duniho, is a retired master programmer with many decades of experience at the National Security Agency. He confirmed that the risk of novel attacks on computer systems is an ever-present threat. Defendant's witnesses opined that disclosure of a mdb file was the

equivalent of making public the architectural drawings of a building. Whatever the merits of the security system that might be in place, unlimited access to the drawings increases the likelihood that a potential intruder could find and exploit a security flaw not known by those responsible for security.

Although it is difficult to quantify an unknown —but plausible — threat, this consideration must be weighed against Plaintiff's interest in the mdb files.

32. Plaintiff does not identify specific reasons why it needs possession of the mdb files. (It previously had asserted the need for audit logs contained within the mdb file that would show alterations and printing of vote tallies prior to the polls closing, but those audit logs have been separately disclosed.) Plaintiff premises its request on two general arguments. The first is based on the presumption in favor of disclosure, which also requires that an official who wishes to withhold public documents must prove specifically how the public interest outweighs this presumption. Citing *Phoenix Newspapers, Inc.v. Keegan*, 201 Ariz. 344, 349 (App. 2001). Second, Plaintiff argues that it cannot perform its statutorily-mandated role of elections monitor unless it can inspect the mdb files.

These general arguments arose from its internal research and informational meetings with Pima County election officials. Plaintiff identified a variety of administrative personnel and physical security issues that could compromise an election or call into question the election results. (Plaintiff is careful to note that it is not alleging or even suggesting that prior elections were compromised or fraudulent.) It now wishes to determine if there are weak spots in the elections management software.

Lynne Booth
Judicial Administrative Assistant

33. The risk of a novel attack based on the public disclosure of an mdb file can be assessed in a limited context. Various witnesses testified about the public disclosure of an mdb file from an Alaska election. The witnesses did not know the context of the disclosure and this Court's own legal research does not disclose it; however, newspaper reports from the Anchorage Daily News describe a suit to release the raw election results. *See e.g.*,www.adn.com/news/politics/elections/story/8218154p-8115104c.html (last visited December 13, 2007). Expert and lay witnesses for both parties testified that they had obtained the mdb file on the Internet, and examined it using various methods.

Professor King also knew of the Alaska mdb file, but only recently. The context and implications of how he learned about this development are revealing. Professor King is the Executive Director of the Center For Election Systems at Kennesaw State University in Georgia. He consults nation-wide with state and federal elections officials about election software. He has a particular interest in security issues. He also oversees a staff of persons at his Center that regularly search for emerging issues in elections management software.

Professor King was not aware of the public disclosure of the Alaska mdb file until his recent involvement with this case. He asked his staff to research the security implications arising from the disclosure of the file. Apparently, despite public disclosure of the Alaska mdb file more than a year ago, it had not registered as a security issue with him or his staff. He testified that there is no indication that the release of the mdb file compromised a subsequent election in Alaska or in any other place in the country.

Professor King opined, however, that the release of a single mdb file may not be sufficient to allow computer hackers to obtain enough information about the architecture of the mdb database to compromise elections in other jurisdictions. He explained that multiple mdb files from various jurisdictions might be necessary to provide confirming data that would enable a computer hacker to map the structure of the GEMS-created mdb file. Essentially, unless multiple copies of mdb files are released it will not be possible to know the actual risk from computer hackers.

Plaintiff's expert witnesses opined that there is nothing in multiple copies of the mdb files that would be of such incremental value that there would be an increased risk if Pima County disclosed all its mdb files. Plaintiff's experts are extremely knowledgeable in computer security and computer programming, but none of them have the hands-on experience with the GEMS program possessed by Defendant's witnesses.

33. The Court finds that the risk of releasing multiple, but not identical, versions of a database file with a similar structure poses a known risk that hackers could use the files to contaminate valid mdb files. The risk arising from the release of mdb files has not been quantified or assessed with any precision. This known-but-unquantified risk, coupled with the possibility of failure in the physical security of elections equipment, cautions against unlimited release of mdb files. The Court concludes

that releasing a large number of mdb files at this time does not protect the interest of the State in valid elections.

The absence of negative consequences from the release of the Alaska mdb file indicates that a limited release of mdb files may not harm the State's interest, or that the reduced risk from disclosure is outweighed by the benefit to the public.

Plaintiff has demonstrated that its participation in monitoring computer-based elections has resulted in increased elections security. Mr. Huckelberry has praised and adopted a number of the physical and personnel recommendations made by the Democratic Party. The continuing interest of the Democratic Party in this area has spurred election officials to conduct internal reviews that have resulted in improvements that are independent from the recommendations made by Plaintiff.

The Court concludes that the public interest will benefit from the continued involvement of Plaintiff in reviewing election management software. Without access to at least some of the mdb files, Plaintiff will be constrained in its ability to fulfill its statutorily-mandated role. The positive benefit to the public by Plaintiff's ability to analyze mdb files for two elections in 2006 outweighs the much smaller risk posed by the disclosure to the public.

Lynne Booth
Judicial Administrative Assistant

RULING

ORDER

IT IS ORDERED that the public records request identified in Plaintiff's December 6, 2006 letter, Item no. 1, is ***granted***. Specifically, Pima County shall disclose pursuant to A.R.S. § 39-121.02 the final mdb and gbf files for the 2006 General and Primary Elections.

IT IS FURTHER ORDERED ***denying*** Plaintiff's March 6, 2007 letter request for "every file that ends with the extension gbf or mdb." Such denial is without prejudice to Plaintiff to re-urge the record request after it has had the opportunity to study the mdb files for the 2006 elections and to address the current (and any future) security concerns raised by Pima County arising from the disclosure of many mdb and gbf files.

Dated this 18th day of December 2007

Michael O. Miller
Judge Michael Miller

cc: Hon. Michael Miller
Willliam J. Risner, Esq./Kenneth K. Graham, Esq. – Risner & Graham
County Attorney – Civil Division – Christopher Straub, Esq./Thomas A. Denker, Esq.

Lynne Booth
Judicial Administrative Assistant